T09040 T6824860

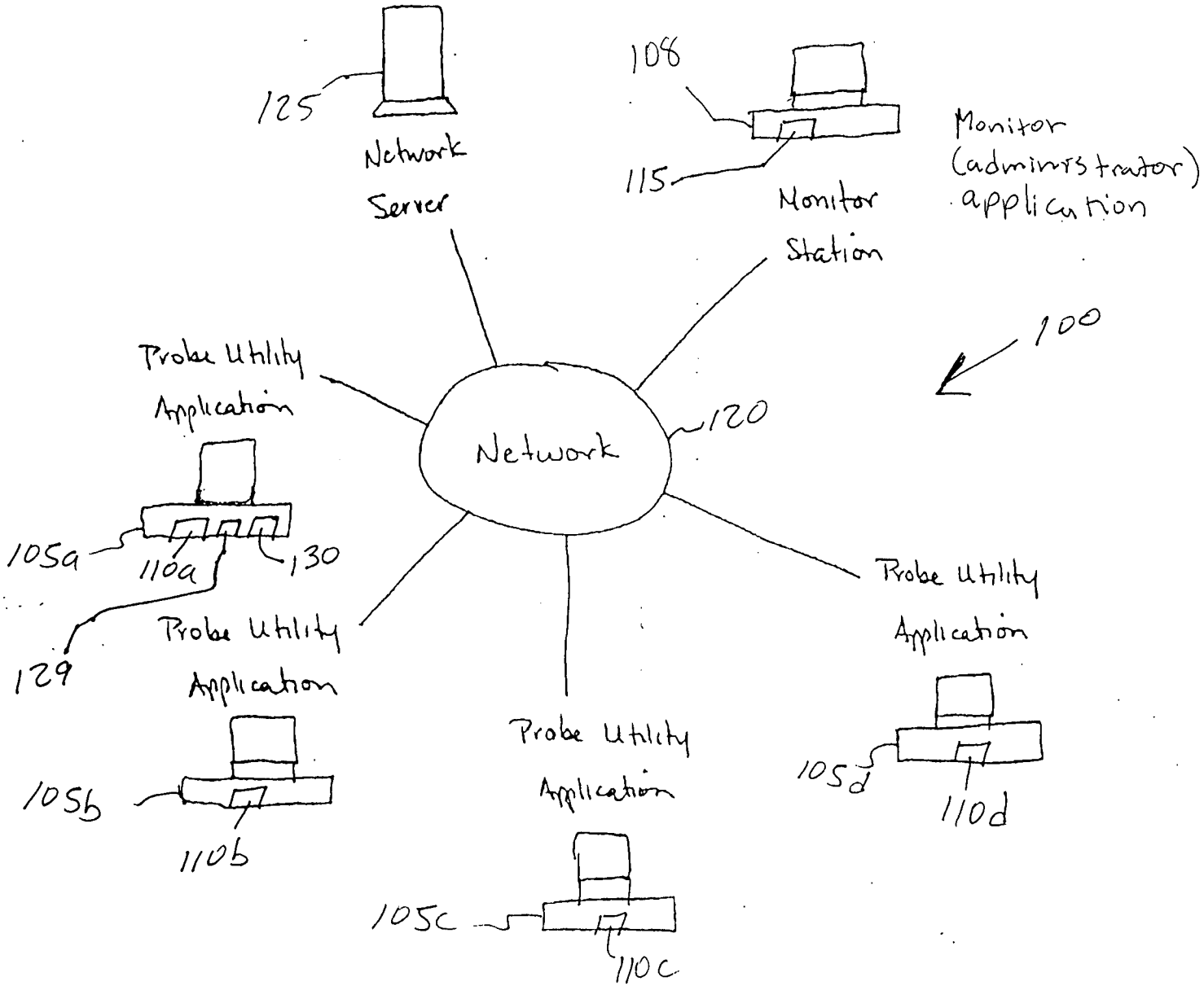


FIG. 1

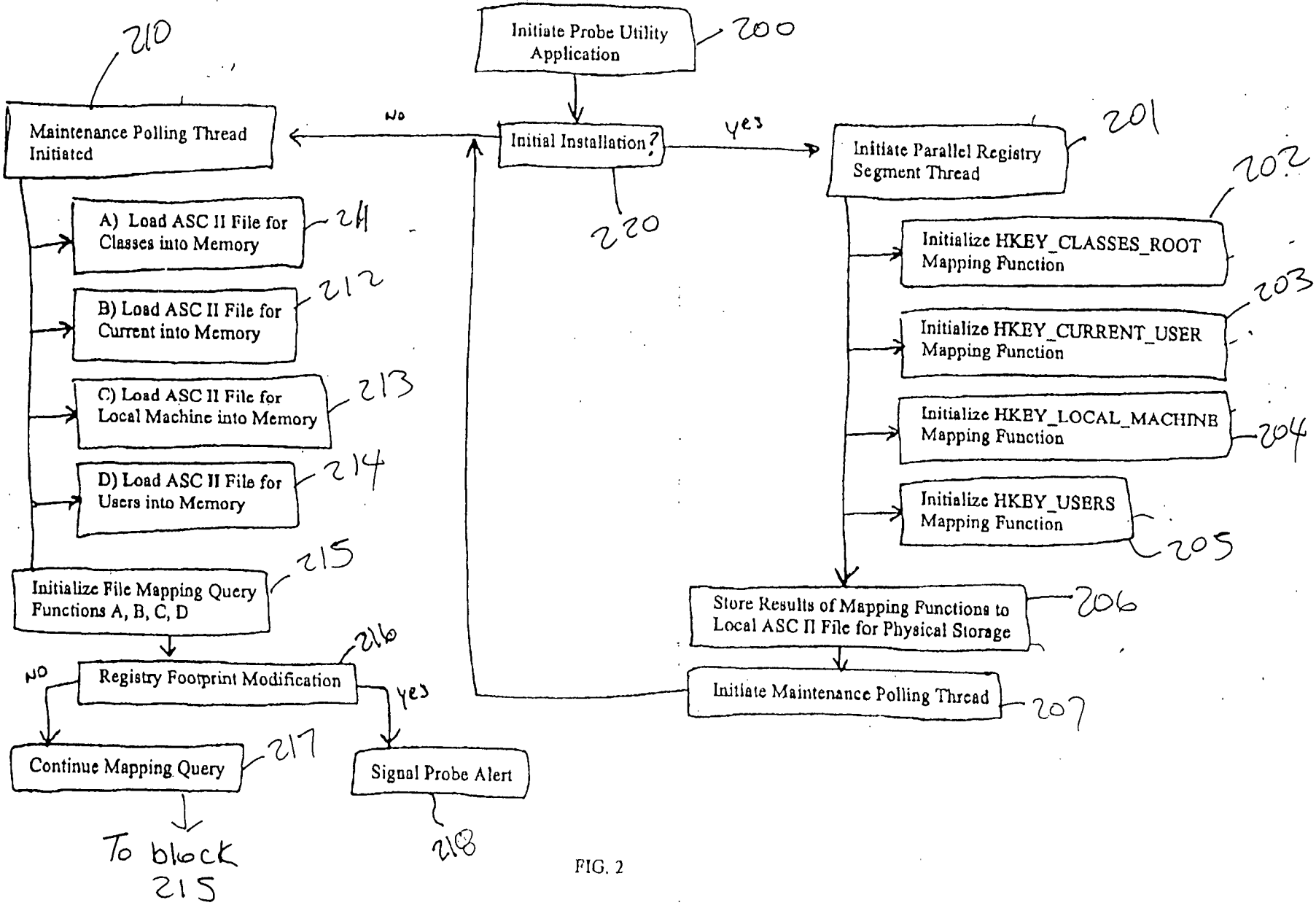

Initiate Probe Utility Application
200
Initial Installation?
220
No
Yes
Maintenance Polling Thread Initiated
210
Initiate Parallel Registry Segment Thread
201
A) Load ASC II File for Classes into Memory
211
B) Load ASC II File for Current into Memory
212
C) Load ASC II File for Local Machine into Memory
213
D) Load ASC II File for Users into Memory
214
Initialize HKEY_CLASSES_ROOT Mapping Function
202
Initialize HKEY_CURRENT_USER Mapping Function
203
Initialize HKEY_LOCAL_MACHINE Mapping Function
204
Initialize HKEY_USERS Mapping Function
205
Initialize File Mapping Query Functions A, B, C, D
215
Store Results of Mapping Functions to Local ASC II File for Physical Storage
206
Registry Footprint Modification
216
No
Yes
Initiate Maintenance Polling Thread
207
Continue Mapping Query
217
Signal Probe Alert
218
To block 215

FIG. 2

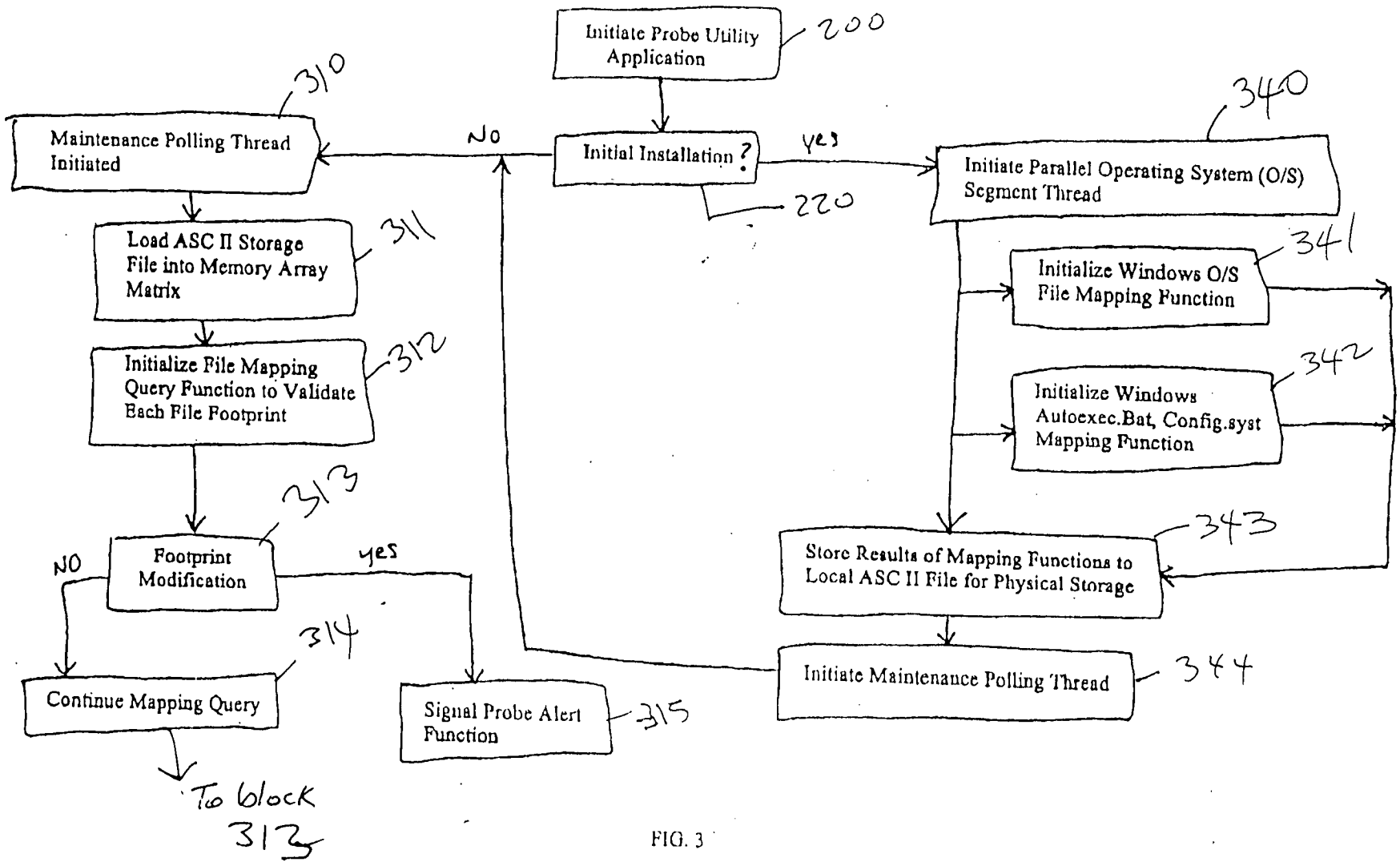

Initiate Probe Utility Application
200
Initial Installation ?
No
yes
220
Maintenance Polling Thread Initiated
310
Load ASC II Storage File into Memory Array Matrix
311
Initialize File Mapping Query Function to Validate Each File Footprint
312
Footprint Modification
313
NO
yes
Continue Mapping Query
314
To block 313
Signal Probe Alert Function
315
Initiate Parallel Operating System (O/S) Segment Thread
340
Initialize Windows O/S File Mapping Function
341
Initialize Windows Autoexec.Bat, Config.syst Mapping Function
342
Store Results of Mapping Functions to Local ASC II File for Physical Storage
343
Initiate Maintenance Polling Thread
344

FIG. 3

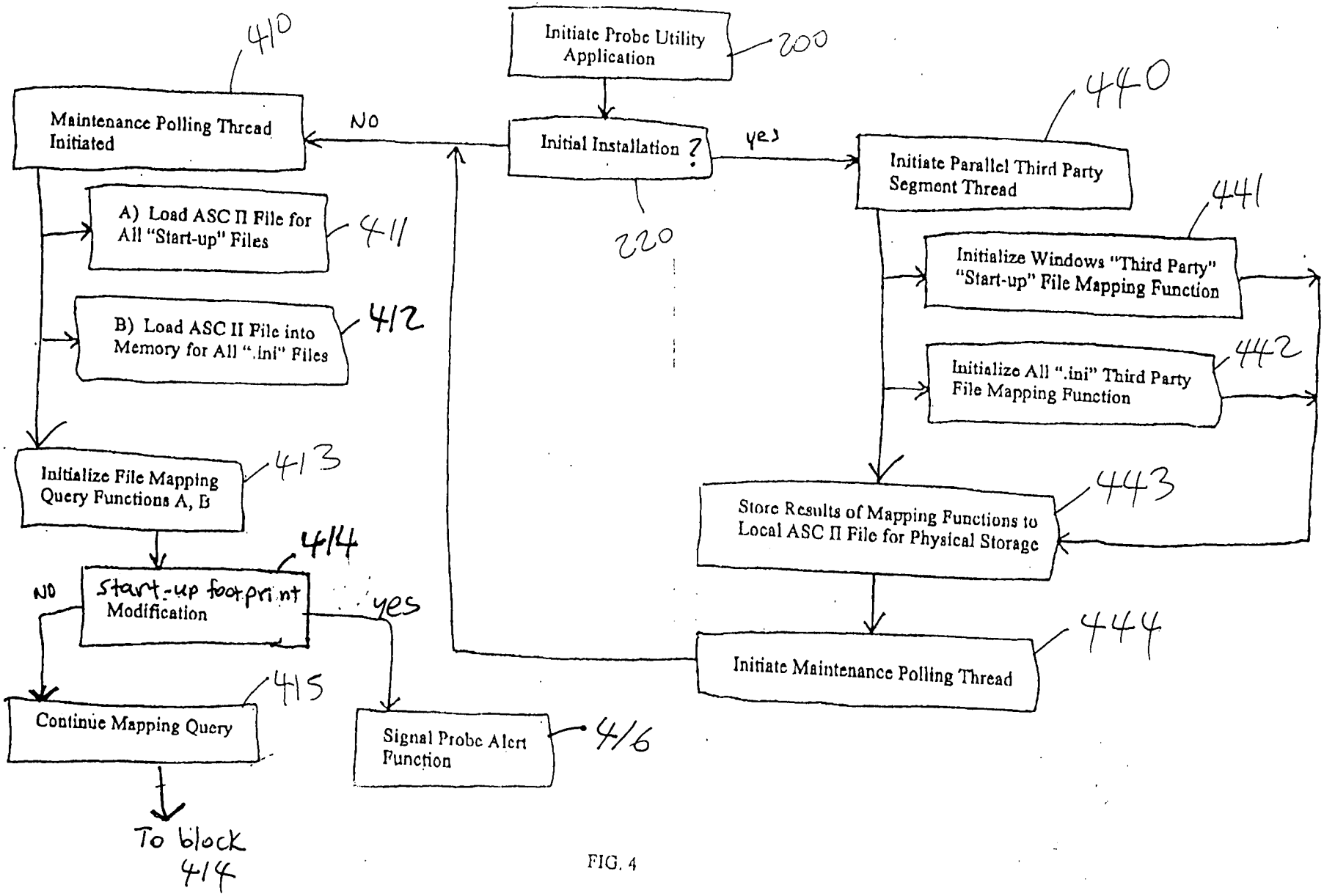

Initiate Probe Utility Application
200
Initial Installation ?
220
NO
yes
Maintenance Polling Thread Initiated
410
A) Load ASC II File for All "Start-up" Files
411
B) Load ASC II File into Memory for All ".ini" Files
412
Initialize File Mapping Query Functions A, B
413
Start-up footprint Modification
414
NO
yes
Continue Mapping Query
415
To block 414
Signal Probe Alert Function
416
Initiate Parallel Third Party Segment Thread
440
Initialize Windows "Third Party" "Start-up" File Mapping Function
441
Initialize All ".ini" Third Party File Mapping Function
442
Store Results of Mapping Functions to Local ASC II File for Physical Storage
443
Initiate Maintenance Polling Thread
444

FIG. 4

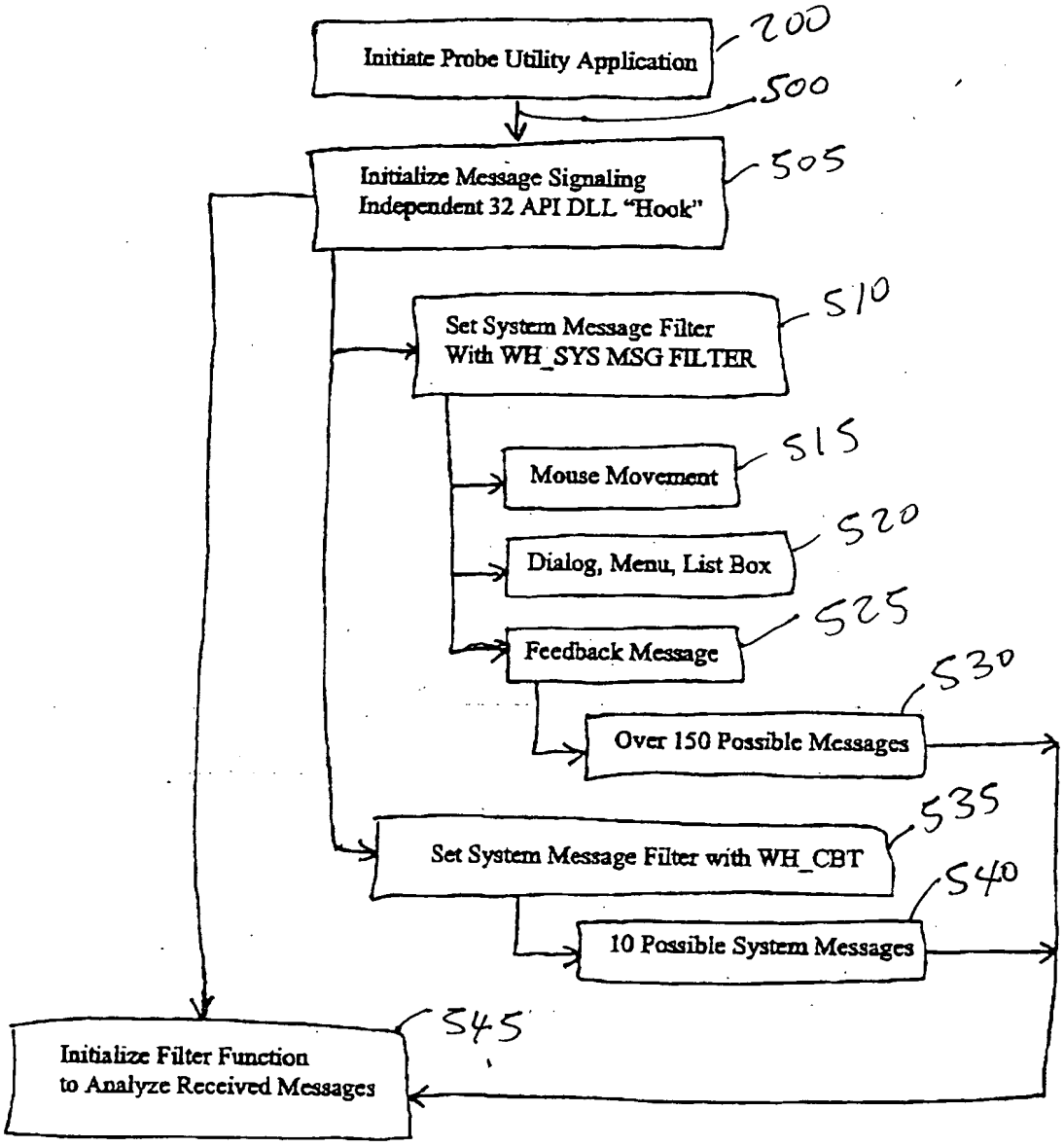

Initiate Probe Utility Application
200
500
Initialize Message Signaling Independent 32 API DLL "Hook"
505
Set System Message Filter With WH_SYS MSG FILTER
510
Mouse Movement
515
Dialog, Menu, List Box
520
Feedback Message
525
Over 150 Possible Messages
530
Set System Message Filter with WH_CBT
535
10 Possible System Messages
540
Initialize Filter Function to Analyze Received Messages
545

FIG. 5

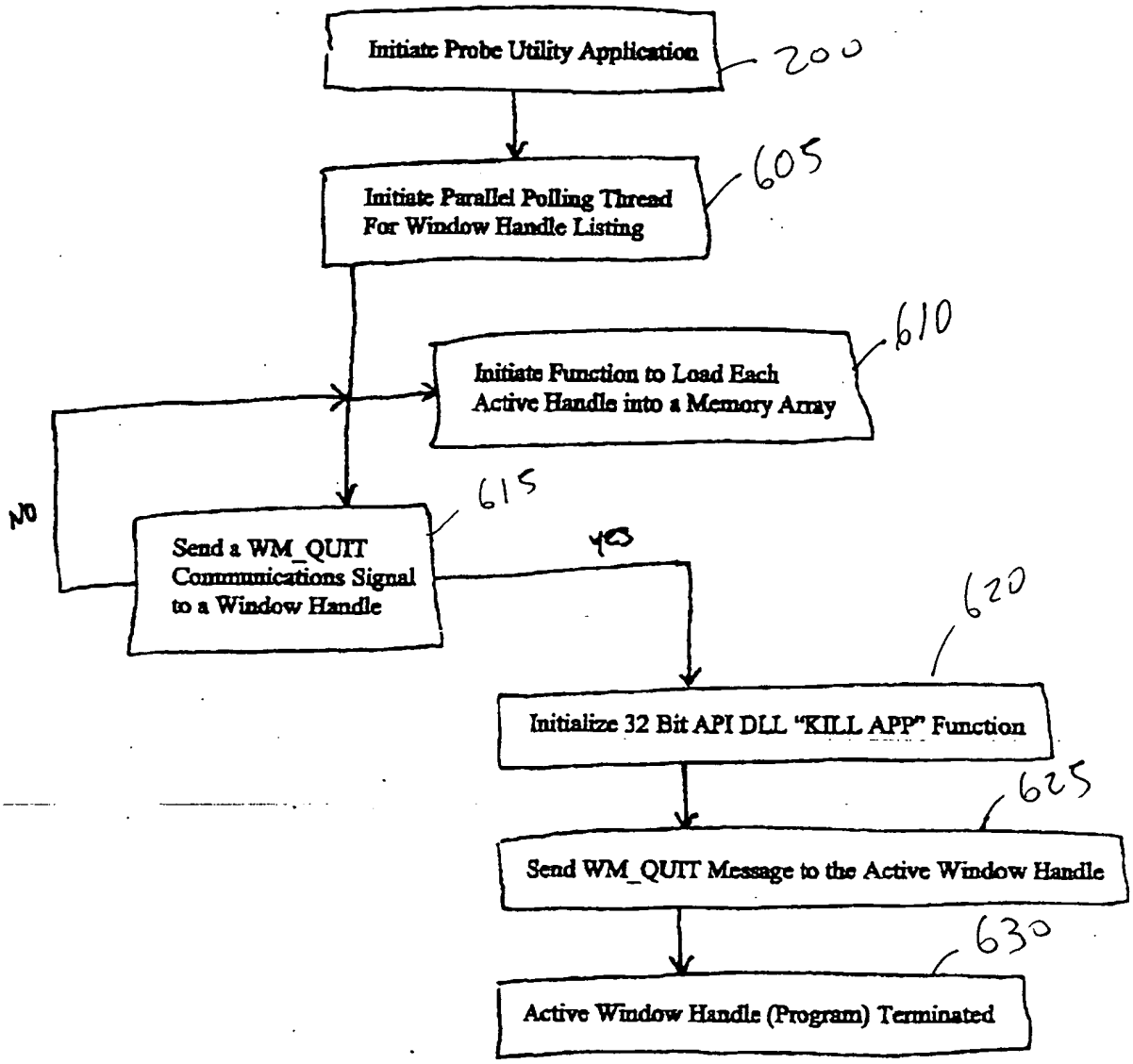

Initiate Probe Utility Application
200
Initiate Parallel Polling Thread For Window Handle Listing
605
Initiate Function to Load Each Active Handle into a Memory Array
610
Send a WM_QUIT Communications Signal to a Window Handle
615
NO
YES
Initialize 32 Bit API DLL "KILL APP" Function
620
Send WM_QUIT Message to the Active Window Handle
625
Active Window Handle (Program) Terminated
630

FIG. 6

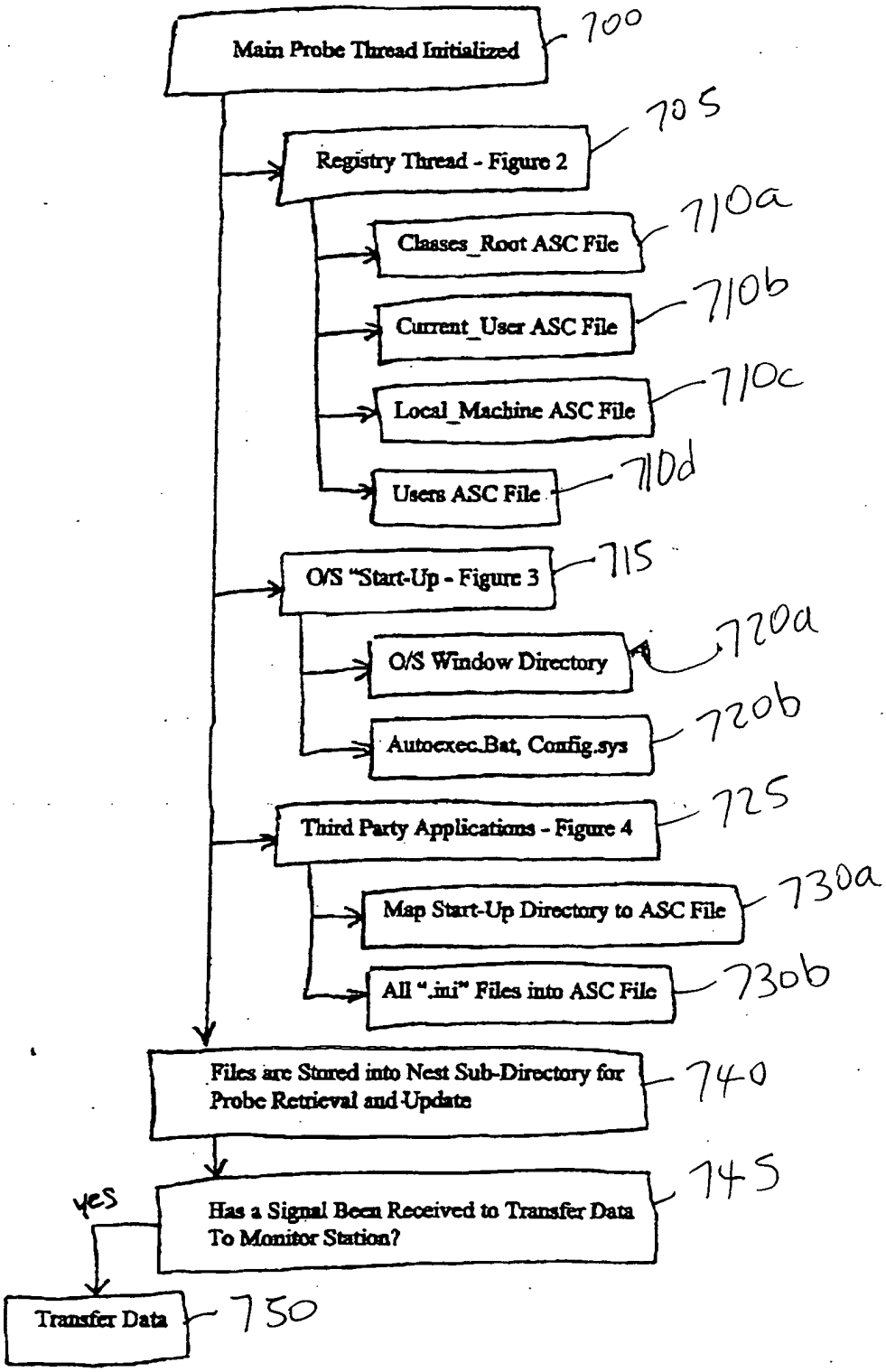

Main Probe Thread Initialized
700
Registry Thread - Figure 2
705
Classes_Root ASC File
710a
Current_User ASC File
710b
Local_Machine ASC File
710c
Users ASC File
710d
O/S "Start-Up - Figure 3
715
O/S Window Directory
720a
Autoexec.Bat, Config.sys
720b
Third Party Applications - Figure 4
725
Map Start-Up Directory to ASC File
730a
All ".ini" Files into ASC File
730b
Files are Stored into Nest Sub-Directory for Probe Retrieval and Update
740
Has a Signal Been Received to Transfer Data To Monitor Station?
745
yes
Transfer Data
750

FIG. 7

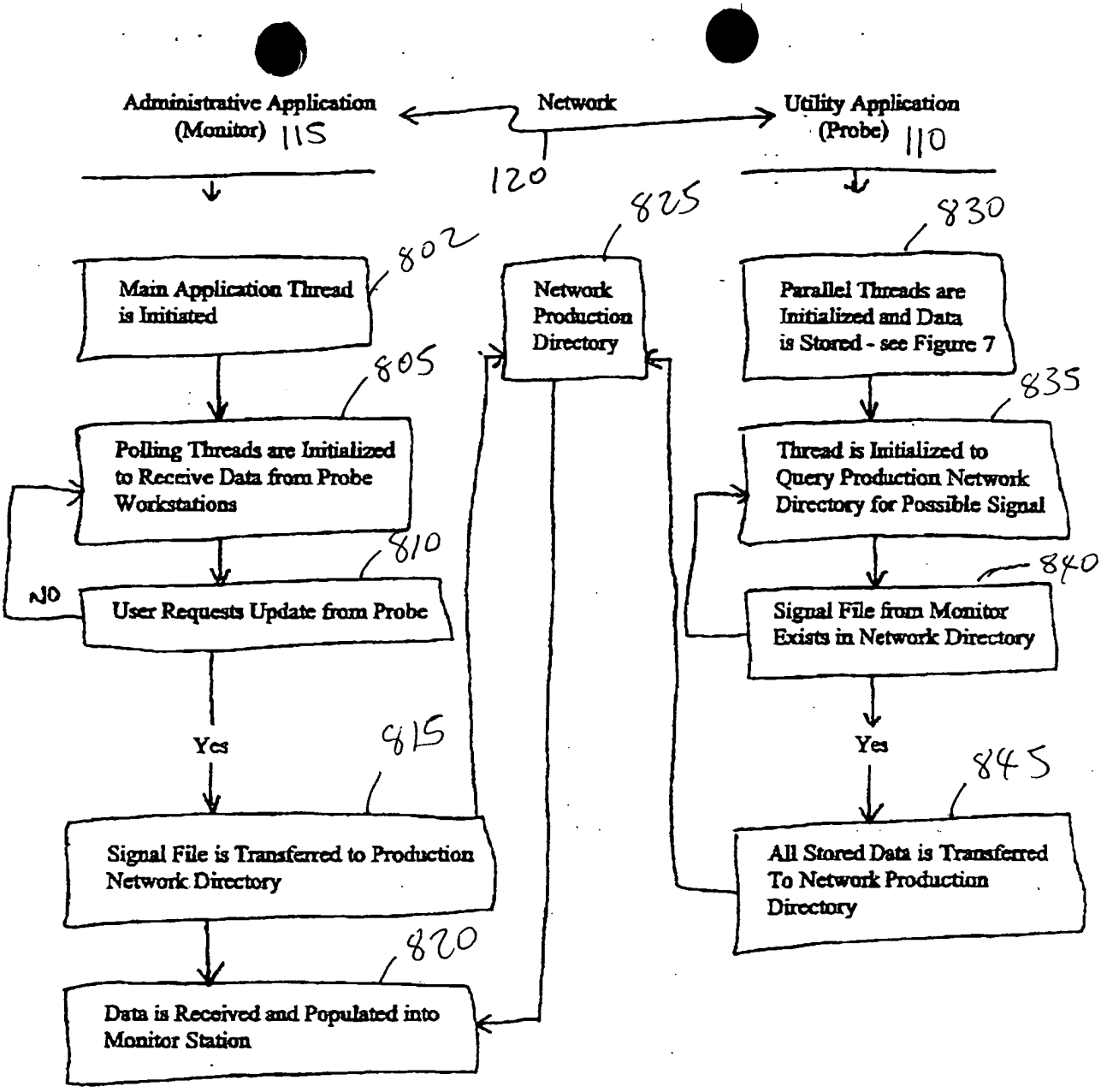

Administrative Application (Monitor) 115
Network
120
Utility Application (Probe) 110
Main Application Thread is Initiated
802
Network Production Directory
825
Parallel Threads are Initialized and Data is Stored - see Figure 7
830
Polling Threads are Initialized to Receive Data from Probe Workstations
805
Thread is Initialized to Query Production Network Directory for Possible Signal
835
User Requests Update from Probe
810
NO
Signal File from Monitor Exists in Network Directory
840
Yes
815
Yes
845
Signal File is Transferred to Production Network Directory
All Stored Data is Transferred To Network Production Directory
Data is Received and Populated into Monitor Station
820

FIG. 8

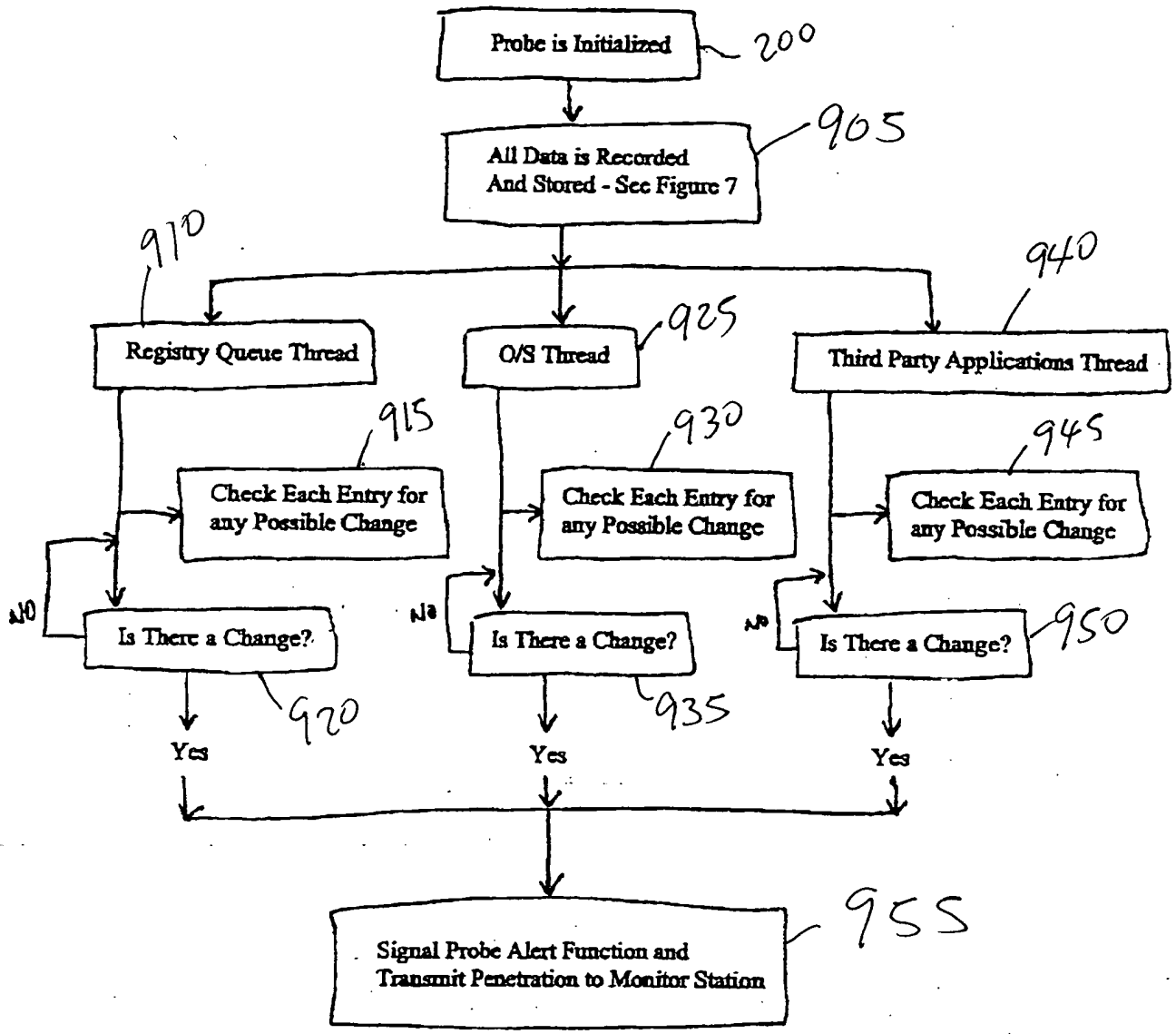

Probe is Initialized
200
All Data is Recorded And Stored - See Figure 7
905
910
940
Registry Queue Thread
O/S Thread
925
Third Party Applications Thread
915
930
945
Check Each Entry for any Possible Change
Check Each Entry for any Possible Change
Check Each Entry for any Possible Change
NO
NO
NO
Is There a Change?
Is There a Change?
Is There a Change?
950
920
935
Yes
Yes
Yes
Signal Probe Alert Function and Transmit Penetration to Monitor Station
955

FIG. 9

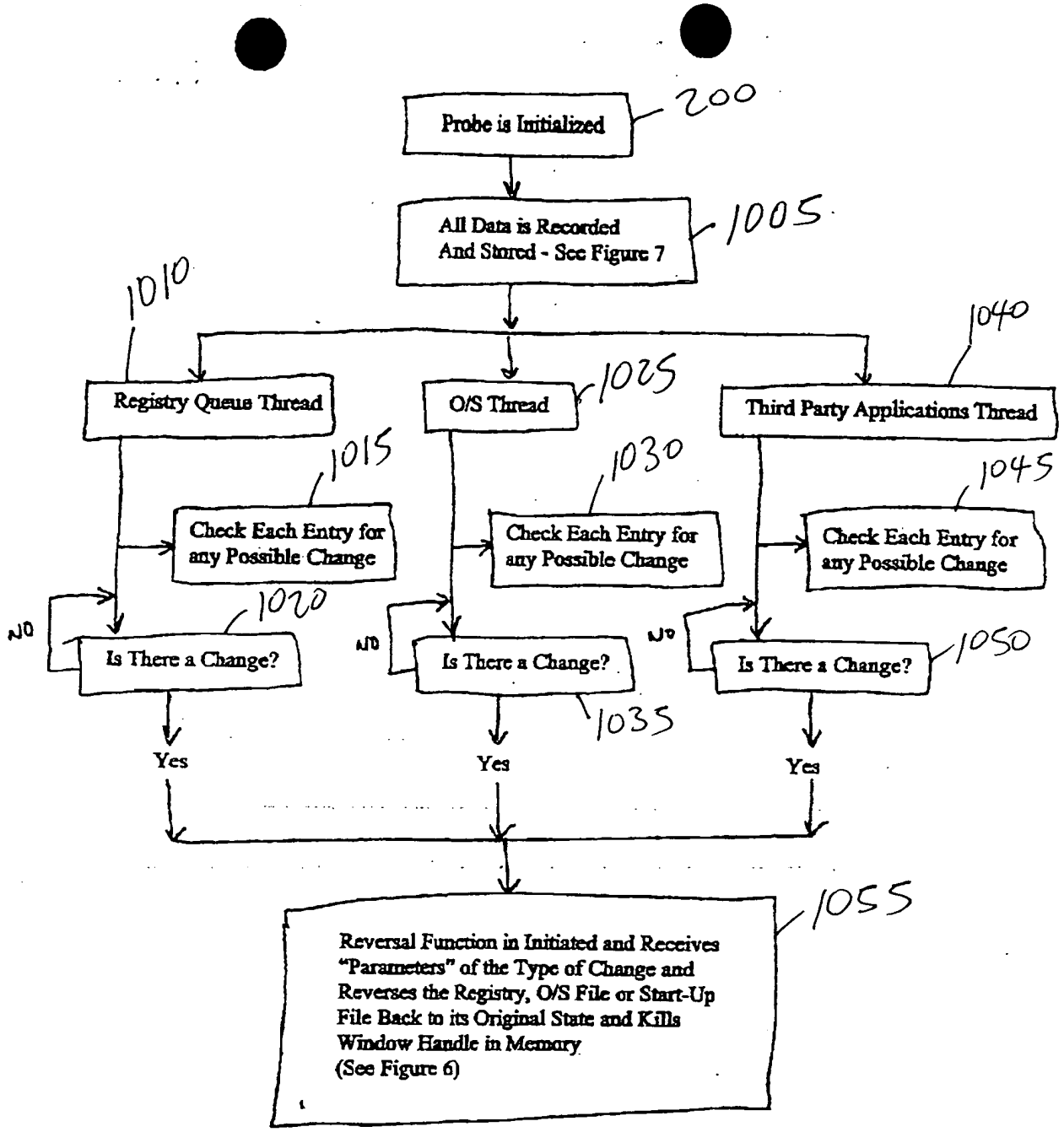
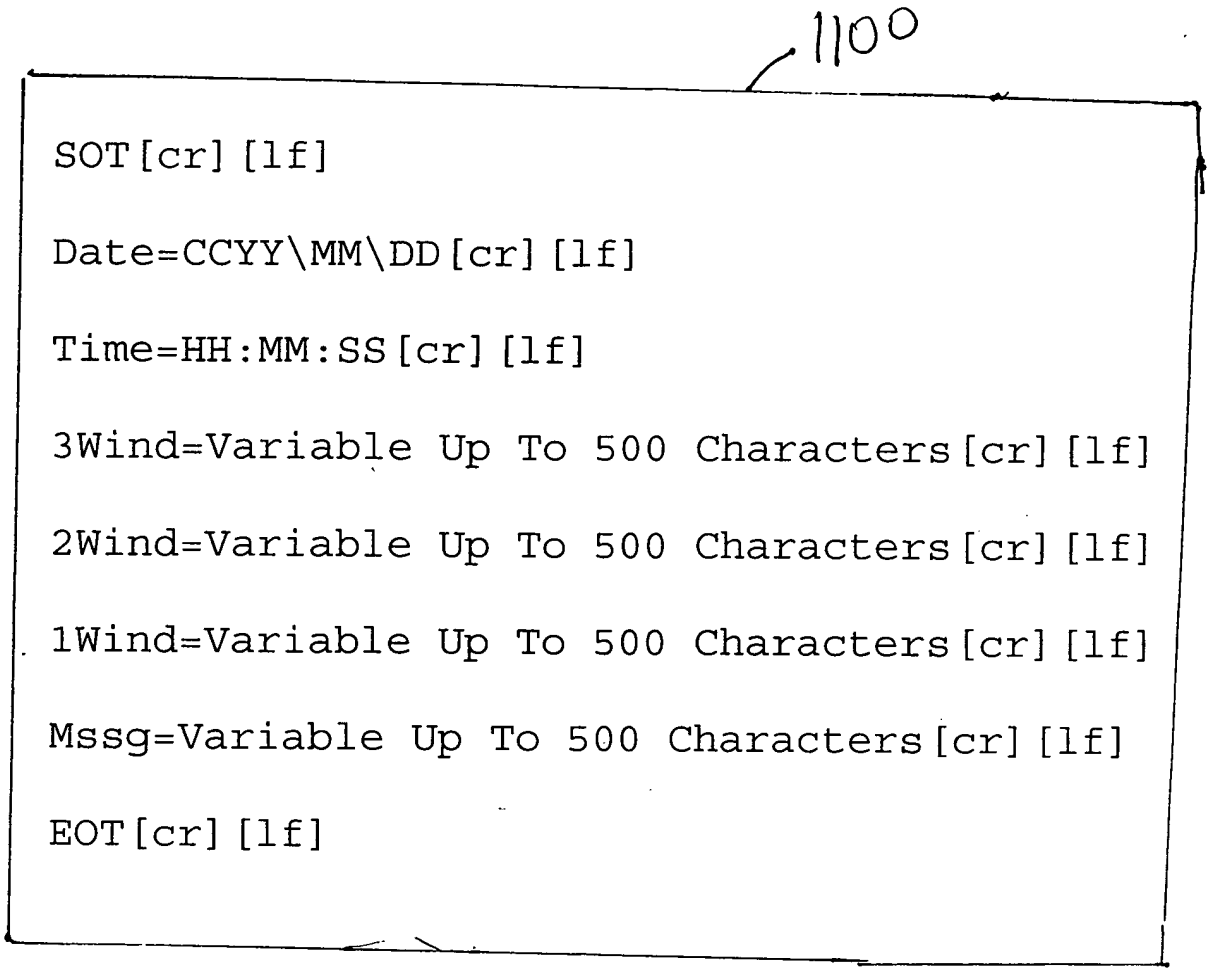

Probe is Initialized
200
All Data is Recorded And Stored - See Figure 7
1005
1010
Registry Queue Thread
O/S Thread
1025
1040
Third Party Applications Thread
1015
Check Each Entry for any Possible Change
1030
Check Each Entry for any Possible Change
1045
Check Each Entry for any Possible Change
1020
NO
Is There a Change?
NO
Is There a Change?
1035
NO
Is There a Change?
1050
Yes
Yes
Yes
1055
Reversal Function in Initiated and Receives "Parameters" of the Type of Change and Reverses the Registry, O/S File or Start-Up File Back to its Original State and Kills Window Handle in Memory
(See Figure 6)

FIG. 10



Structured Signal File Block Diagram

Figure 11

Express Mail No. EV 369 469 649

Figure 12

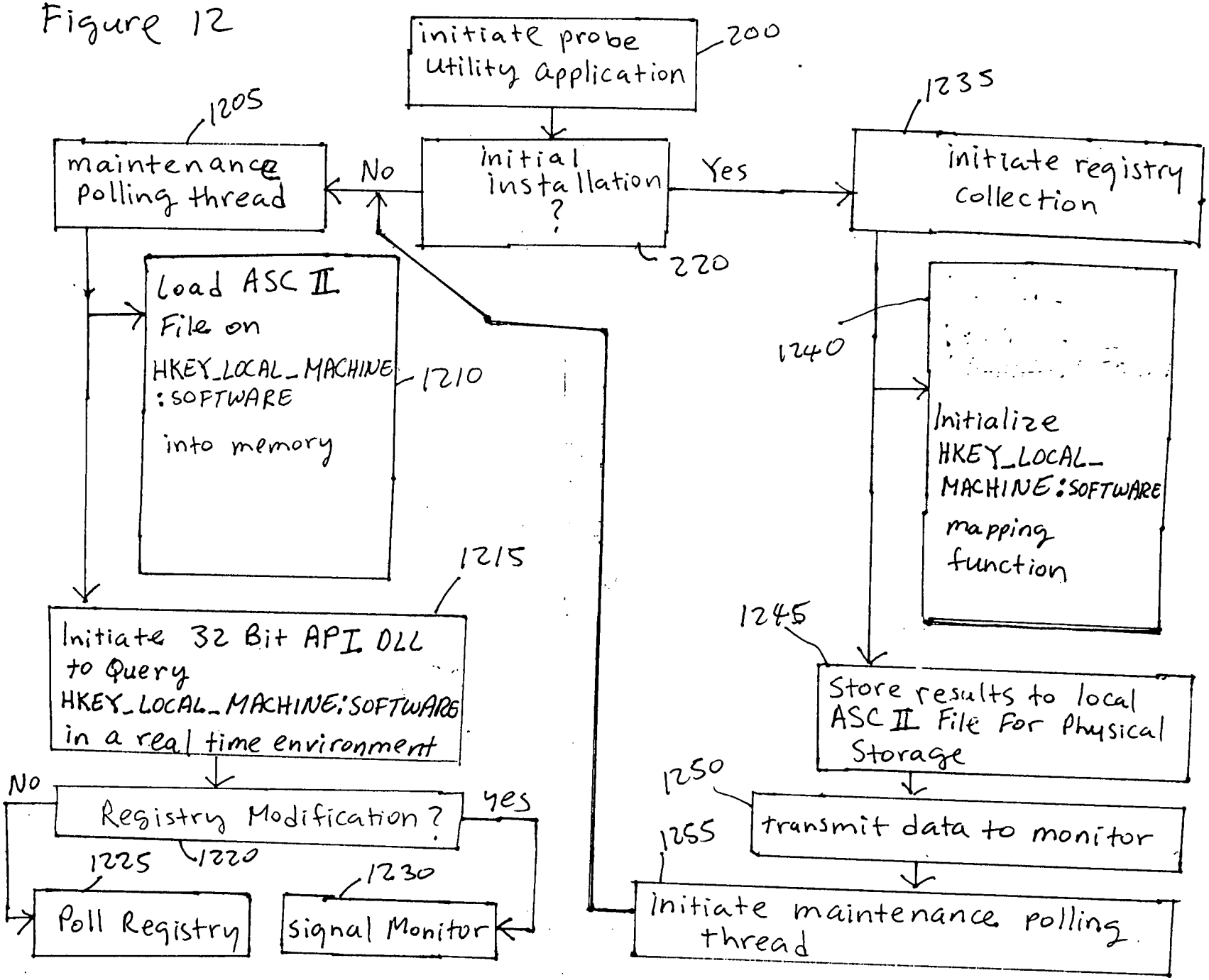

initiate probe utility application
200
initial installation ?
No
Yes
220
maintenance polling thread
1205
Load ASC II File on HKEY_LOCAL_MACHINE:SOFTWARE into memory
1210
Initiate 32 Bit API DLL to Query HKEY_LOCAL_MACHINE:SOFTWARE in a real time environment
1215
Registry Modification ?
No
yes
1220
Poll Registry
1225
signal Monitor
1230
initiate registry collection
1235
1240
Initialize HKEY_LOCAL_MACHINE:SOFTWARE mapping function
Store results to local ASC II File For Physical Storage
1245
transmit data to monitor
1250
Initiate maintenance polling thread
1255

Figure 13

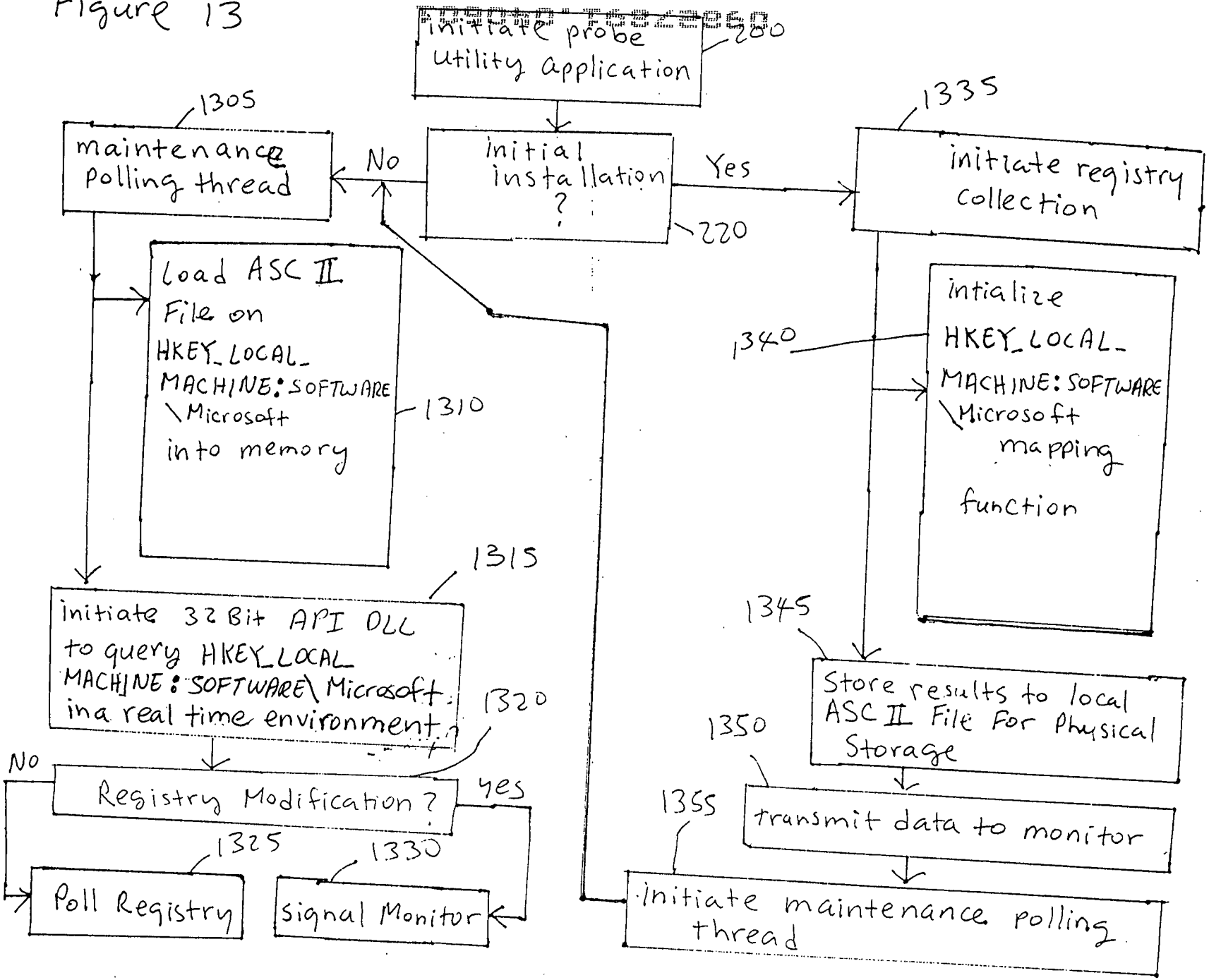

initiate probe utility application
200
initial installation ?
220
No
Yes
1305
maintenance polling thread
1335
initiate registry collection
load ASC II File on HKEY_LOCAL_MACHINE:SOFTWARE\Microsoft into memory
1310
intialize HKEY_LOCAL_MACHINE:SOFTWARE\Microsoft mapping function
1340
1315
initiate 32 Bit API DLL to query HKEY_LOCAL_MACHINE:SOFTWARE\Microsoft in a real time environment
1345
Store results to local ASC II File For Physical Storage
1320
1350
No
Registry Modification ?
yes
1355
transmit data to monitor
1325
1330
Poll Registry
signal Monitor
initiate maintenance polling thread

Figure 14

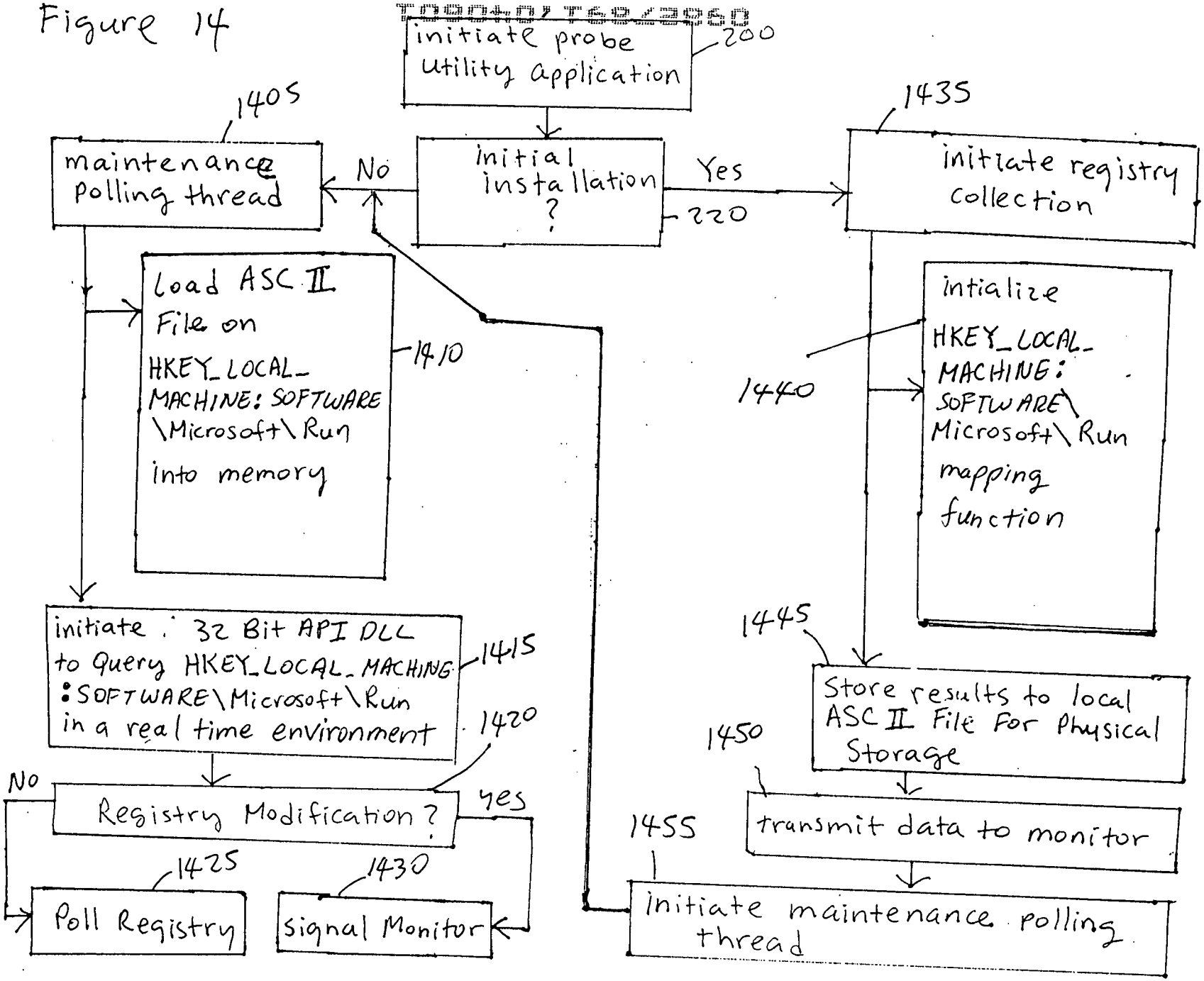

initiate probe utility application
200
initial installation ?
220
No
Yes
maintenance polling thread
1405
initiate registry collection
1435
Load ASC II File on HKEY_LOCAL_MACHINE: SOFTWARE \Microsoft\Run into memory
1410
intialize HKEY_LOCAL_MACHINE: SOFTWARE\Microsoft\Run mapping function
1440
initiate 32 Bit API DLL to Query HKEY_LOCAL_MACHING :SOFTWARE\Microsoft\Run in a real time environment
1415
Store results to local ASC II File For Physical Storage
1445
1450
Registry Modification ?
1420
No
yes
transmit data to monitor
1455
Poll Registry
1425
signal Monitor
1430
initiate maintenance polling thread

Figure 15

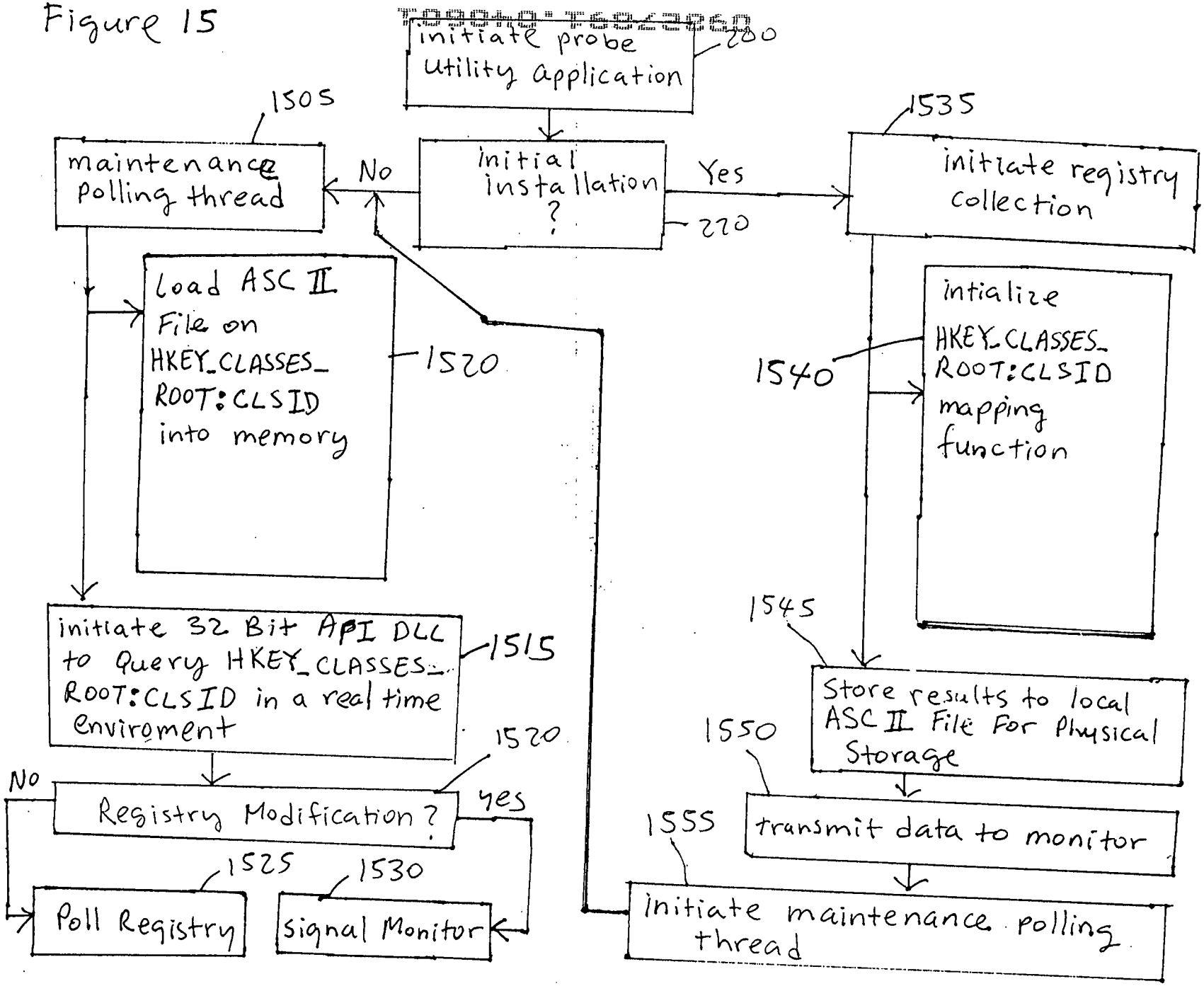

initiate probe utility application
200
initial installation ?
No
Yes
220
1505
maintenance polling thread
1535
initiate registry collection
load ASC II File on HKEY_CLASSES_ROOT:CLSID into memory
1520
intialize HKEY_CLASSES_ROOT:CLSID mapping function
1540
initiate 32 Bit API DLL to Query HKEY_CLASSES_ROOT:CLSID in a real time enviroment
1515
1545
Store results to local ASC II File For Physical Storage
1550
1520
No
Registry Modification ?
yes
transmit data to monitor
1555
1525
1530
Poll Registry
signal Monitor
initiate maintenance polling thread

Figure 16

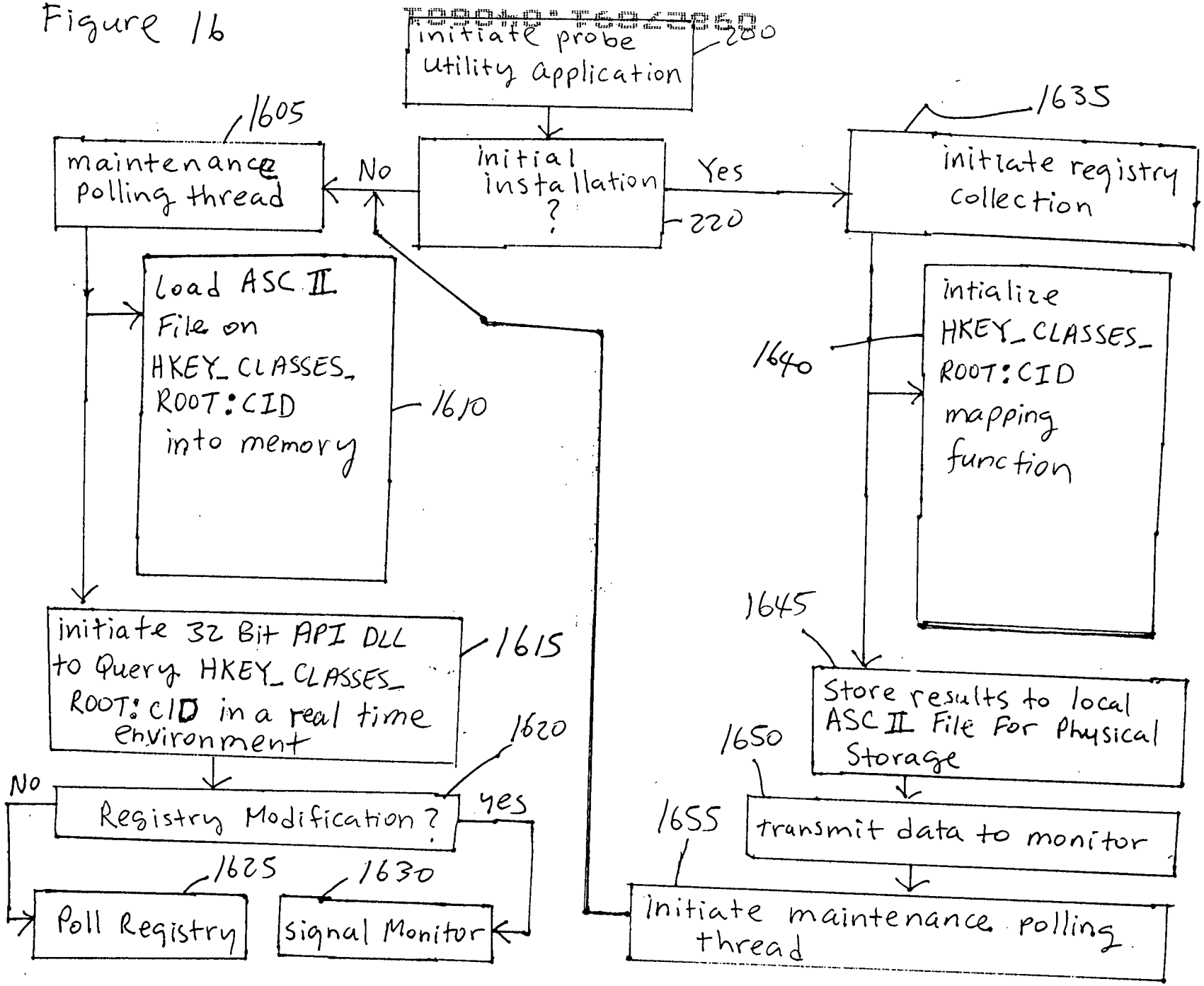

initiate probe utility application
200
initial installation ?
220
No
Yes
maintenance Polling thread
1605
initiate registry collection
1635
Load ASC II File on HKEY_CLASSES_ROOT:CID into memory
1610
intialize HKEY_CLASSES_ROOT:CID mapping function
1640
initiate 32 Bit API DLL to Query HKEY_CLASSES_ROOT:CID in a real time environment
1615
1645
Store results to local ASC II File For Physical Storage
1650
Registry Modification ?
1620
No
yes
transmit data to monitor
1655
Poll Registry
1625
signal Monitor
1630
Initiate maintenance polling thread

Figure 17

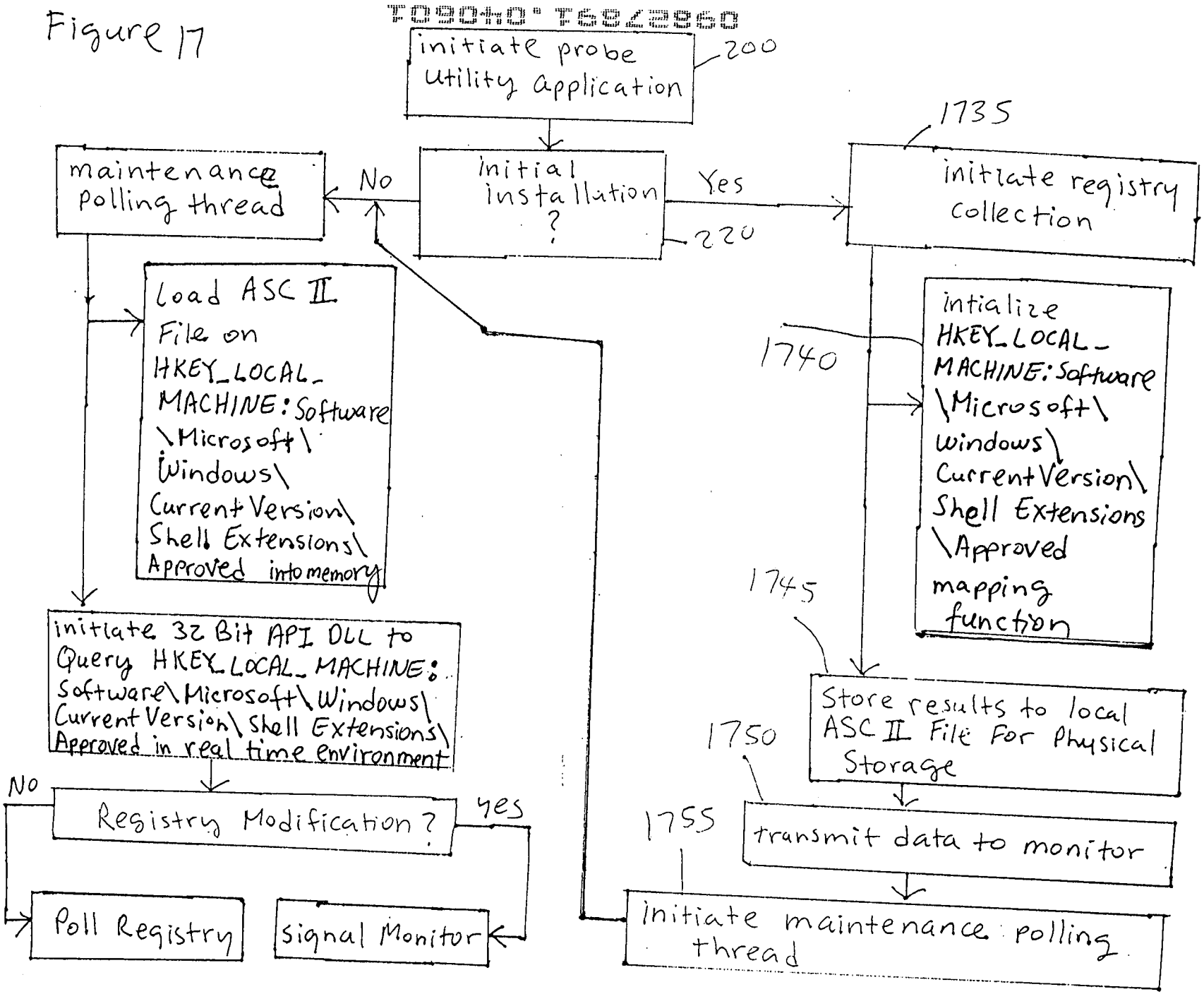

initiate probe utility application
200
initial installation ?
No
Yes
220
maintenance polling thread
1735
initiate registry collection
Load ASC II File on HKEY_LOCAL_MACHINE: Software \Microsoft\ Windows\ CurrentVersion\ Shell Extensions\ Approved into memory
1740
intialize HKEY_LOCAL_MACHINE: Software \Microsoft\ windows\ CurrentVersion\ Shell Extensions \Approved mapping function
1745
initiate 32 Bit API DLL to Query HKEY_LOCAL_MACHINE: Software\Microsoft\Windows\ CurrentVersion\Shell Extensions\ Approved in real time environment
Store results to local ASC II File For Physical Storage
1750
No
Registry Modification ?
yes
1755
transmit data to monitor
Poll Registry
signal Monitor
initiate maintenance polling thread

Figure 18

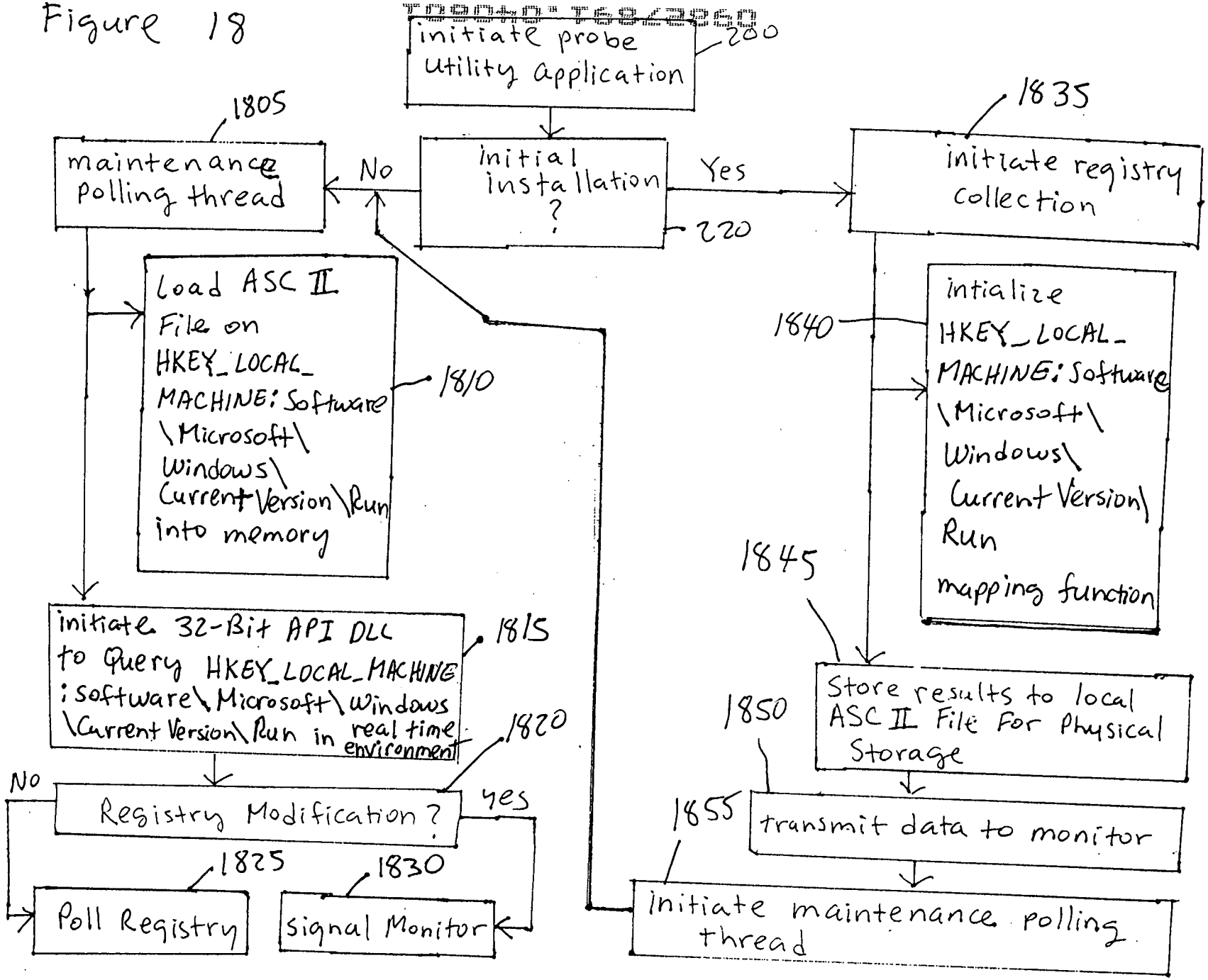

initiate probe utility application
200
initial installation ?
220
No
Yes
maintenance polling thread
1805
initiate registry collection
1835
Load ASC II File on HKEY_LOCAL_MACHINE: Software\Microsoft\Windows\Current Version\Run into memory
1810
intialize HKEY_LOCAL_MACHINE: Software\Microsoft\Windows\Current Version\Run mapping function
1840
initiate 32-Bit API DLL to Query HKEY_LOCAL_MACHINE: Software\Microsoft\Windows\Current Version\Run in real time environment
1815
1845
Store results to local ASC II File For Physical Storage
1850
Registry Modification ?
1820
No
yes
transmit data to monitor
1855
Poll Registry
1825
signal Monitor
1830
initiate maintenance polling thread

Figure 19

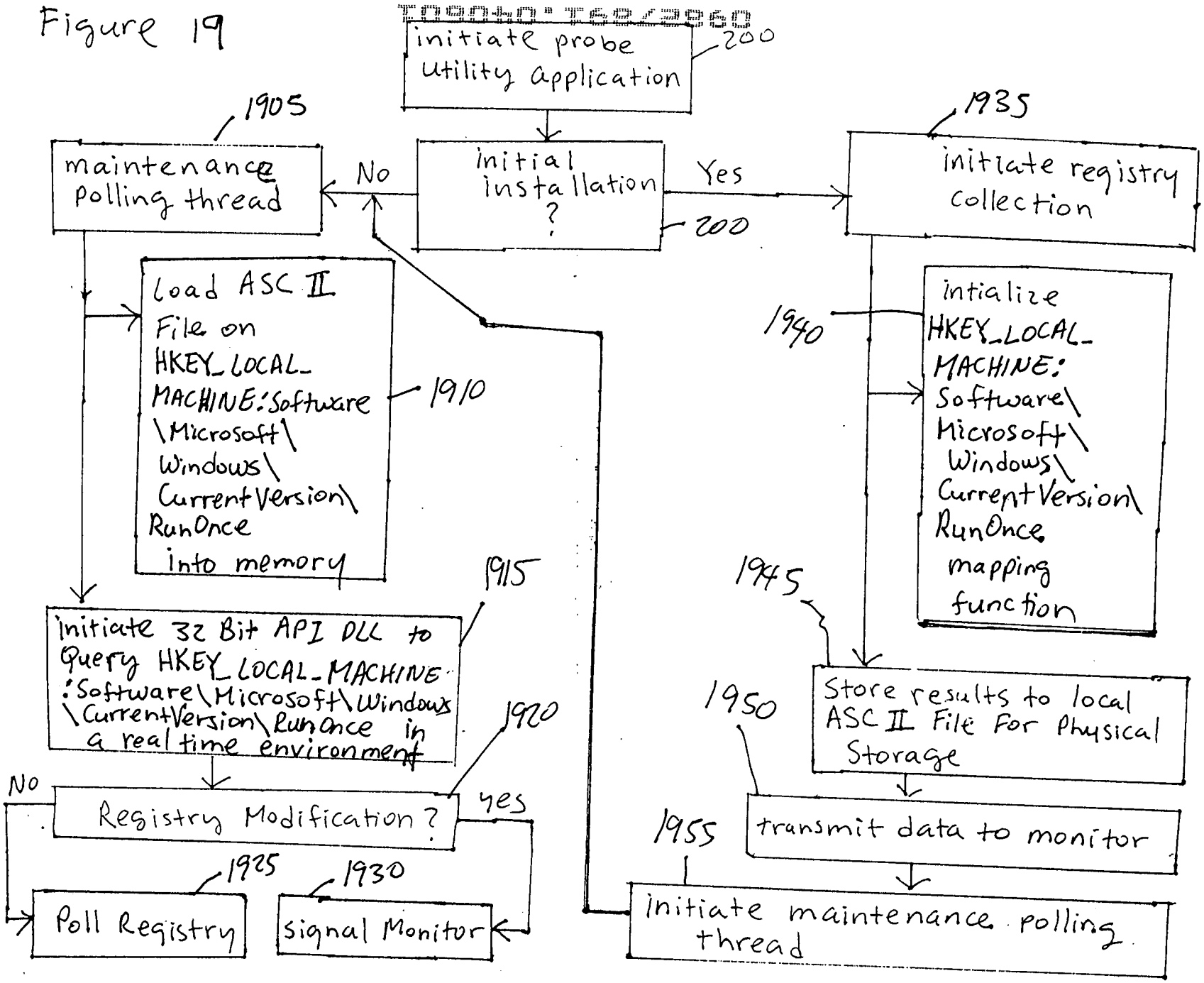

initiate probe utility application
200
initial installation ?
No
Yes
200
1905
maintenance polling thread
1935
initiate registry collection
Load ASC II File on HKEY_LOCAL_MACHINE:Software\Microsoft\Windows\CurrentVersion\RunOnce into memory
1910
intialize HKEY_LOCAL_MACHINE:Software\Microsoft\Windows\CurrentVersion\RunOnce mapping function
1940
1915
Initiate 32 Bit API DLL to Query HKEY_LOCAL_MACHINE:Software\Microsoft\Windows\CurrentVersion\RunOnce in a real time environment
1945
1920
Store results to local ASC II File For Physical Storage
1950
No
Registry Modification ?
yes
1955
transmit data to monitor
1925
1930
Poll Registry
signal Monitor
initiate maintenance polling thread

Figure 20

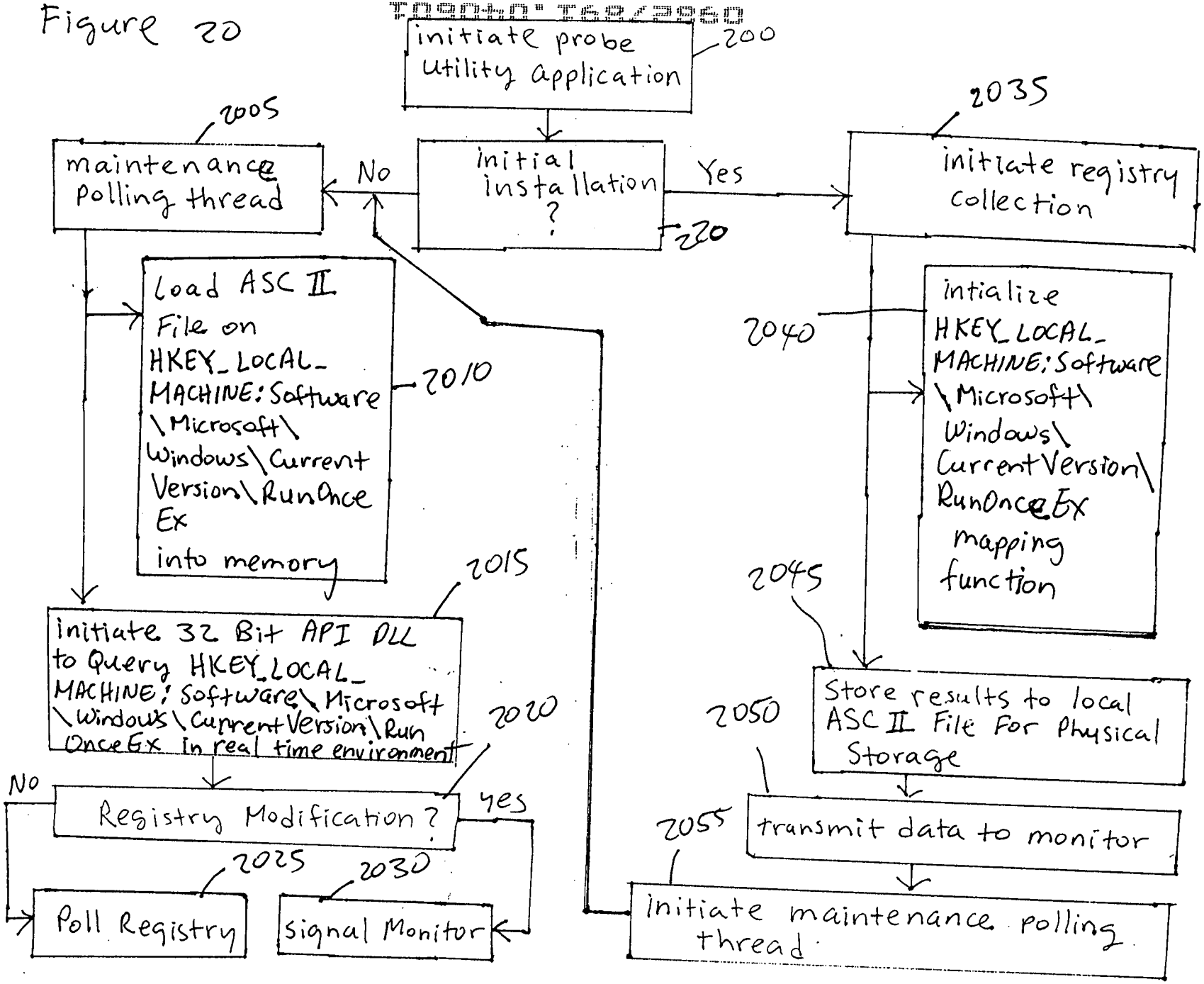
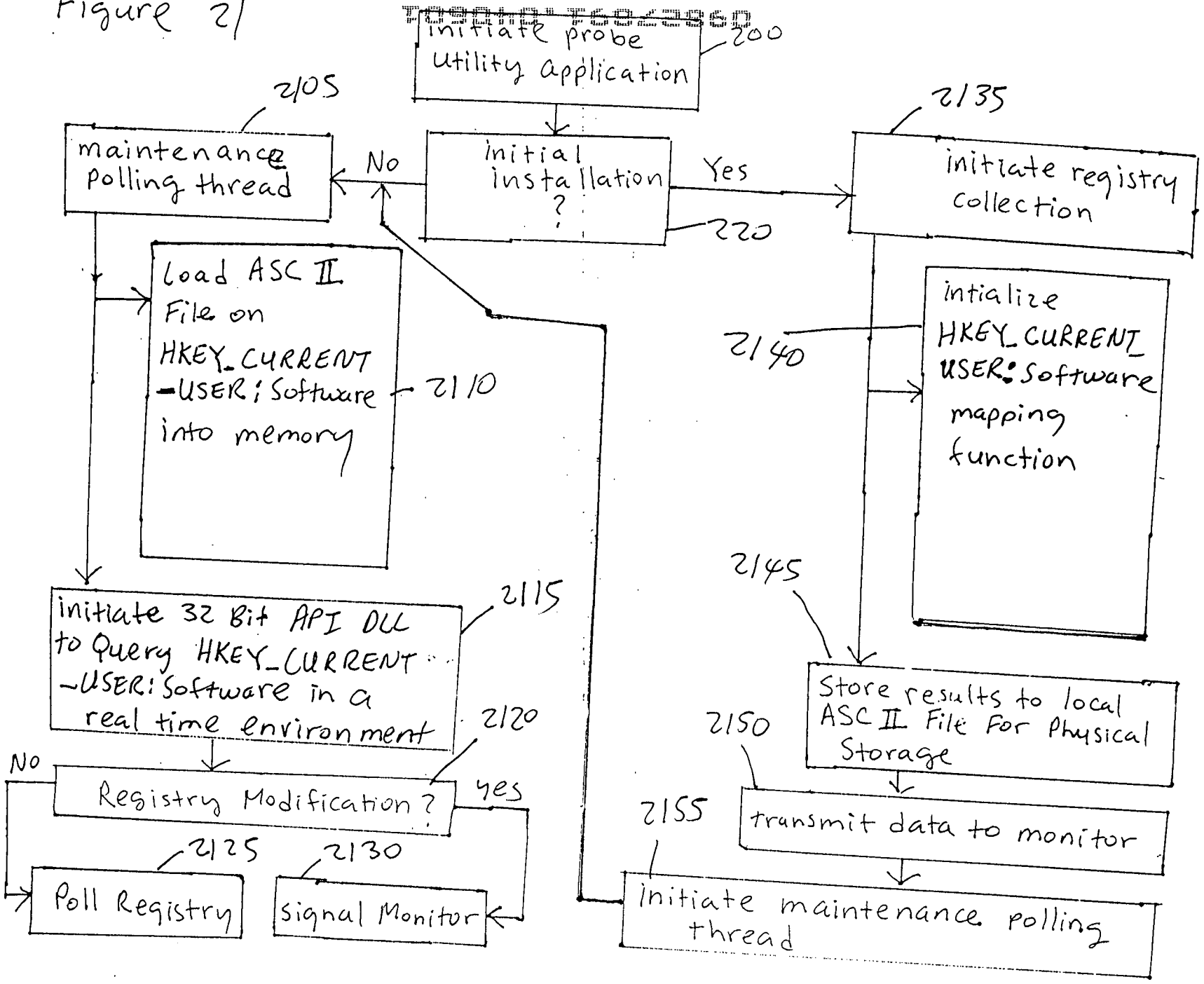
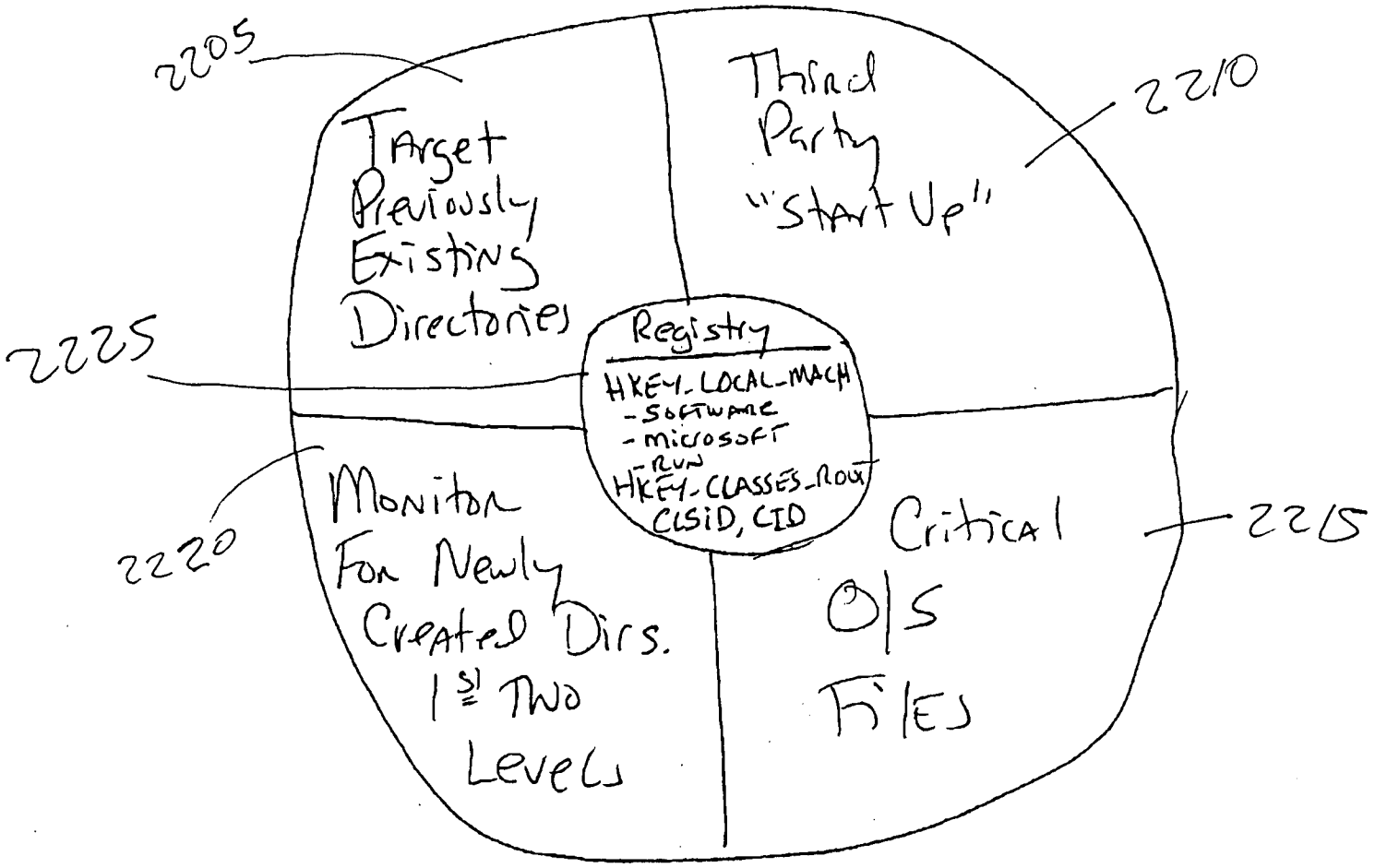

initiate probe utility application
200
initial installation ?
220
No
Yes
maintenance polling thread
2005
Load ASC II File on HKEY_LOCAL_MACHINE:Software\Microsoft\Windows\CurrentVersion\RunOnceEx into memory
2010
initiate 32 Bit API DLL to Query HKEY_LOCAL_MACHINE:Software\Microsoft\Windows\CurrentVersion\RunOnceEx in real time environment
2015
Registry Modification ?
2020
No
yes
Poll Registry
2025
signal Monitor
2030
initiate registry collection
2035
intialize HKEY_LOCAL_MACHINE:Software\Microsoft\Windows\CurrentVersion\RunOnceEx mapping function
2040
Store results to local ASC II File For Physical Storage
2045
transmit data to monitor
2050
initiate maintenance polling thread
2055

Figure 2/


initiate probe utility application
200
initial installation ?
No
Yes
220
maintenance polling thread
2105
initiate registry collection
2135
Load ASC II File on HKEY_CURRENT_USER; Software into memory
2110
intialize HKEY_CURRENT_USER: Software mapping function
2140
initiate 32 Bit API DLL to Query HKEY_CURRENT_USER: Software in a real time environment
2115
Store results to local ASC II File For Physical Storage
2145
2150
Registry Modification ?
2120
No
yes
transmit data to monitor
2155
Poll Registry
2125
signal Monitor
2130
initiate maintenance polling thread

T0904.0" T68.2860

GTI "Defense UmBrellA"



"GAURDED STATE" OF the Complete PC

Figure 22

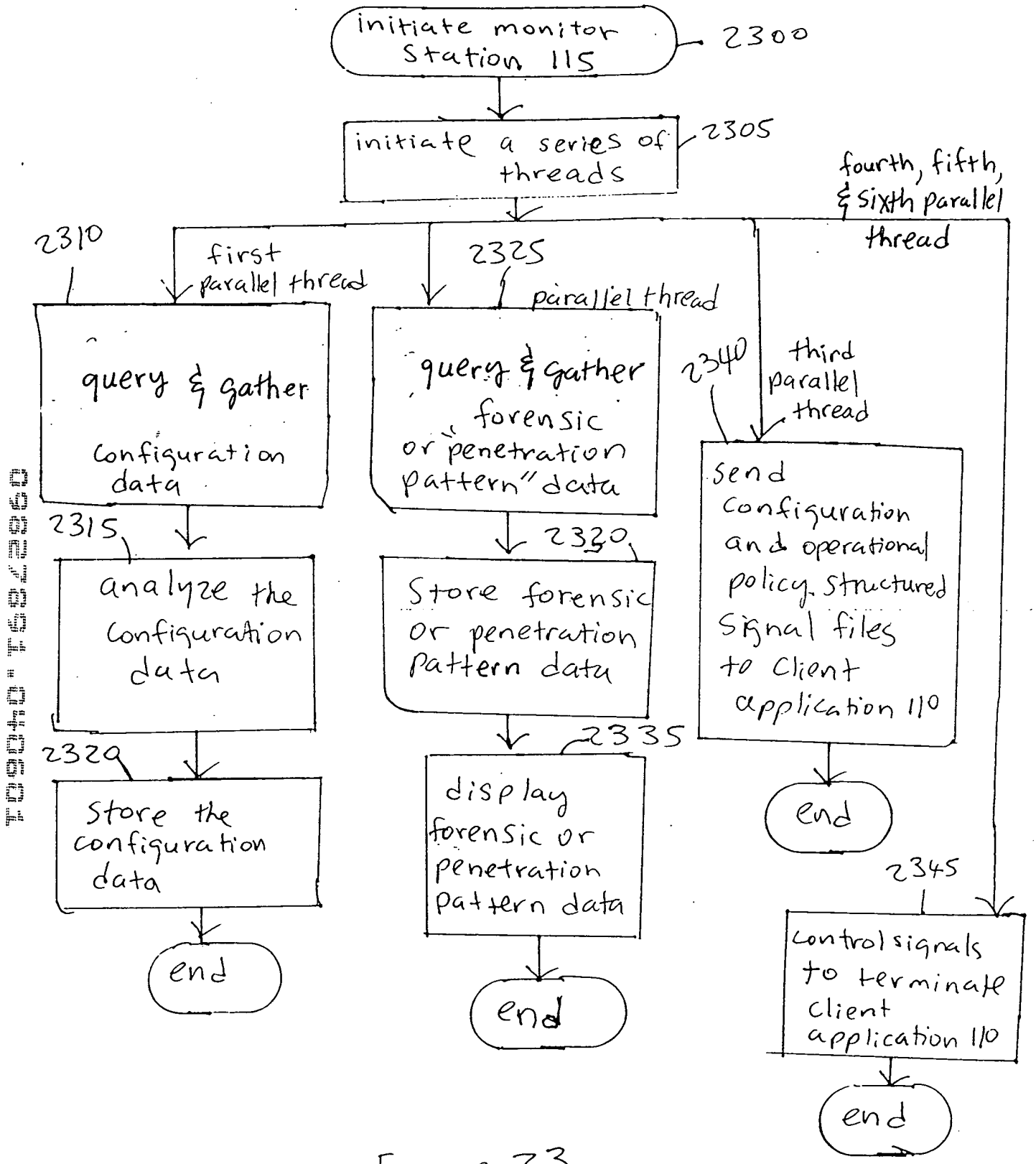

initiate monitor Station 115
2300
initiate a series of threads
2305
fourth, fifth, & sixth parallel thread
2310
first parallel thread
2325
parallel thread
2340
third parallel thread
query & gather configuration data
query & gather forensic or "penetration pattern" data
send configuration and operational policy structured signal files to client application 110
2315
analyze the configuration data
2330
Store forensic or penetration pattern data
2320
Store the configuration data
2335
display forensic or penetration pattern data
2345
control signals to terminate client application 110
end
end
end
end

Figure 23

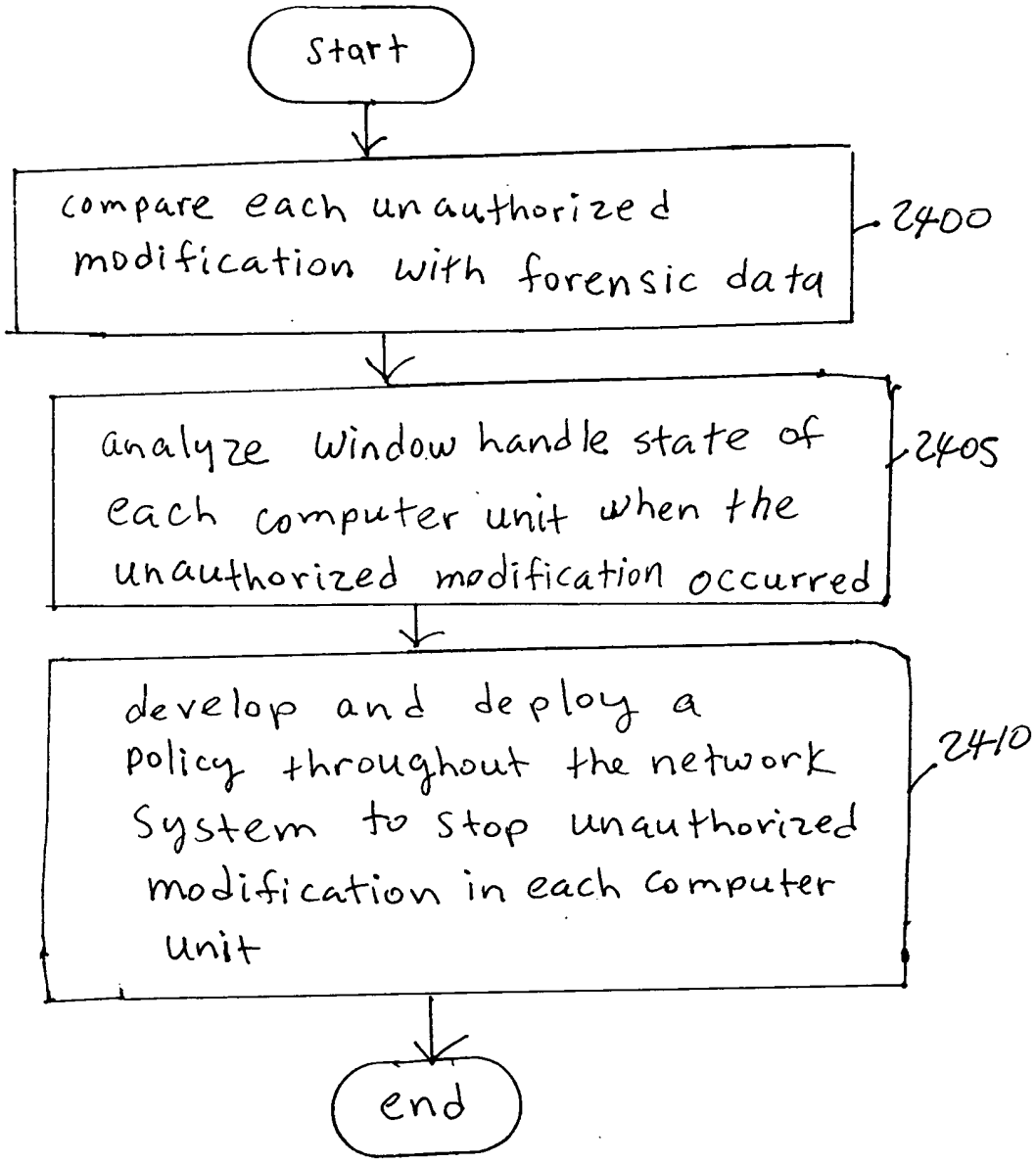

Start
compare each unauthorized modification with forensic data
2400
analyze window handle state of each computer unit when the unauthorized modification occurred
2405
develop and deploy a policy throughout the network System to stop unauthorized modification in each computer unit
2410
end

Figure 24